



IT TECHNOLOGY CHECKLIST

For Small Business Owners in Australia

About This Checklist

Use this checklist to review your current IT setup and identify areas that need attention. Each item includes a simple explanation to help you understand what to consider.

1. INTERNET & CONNECTIVITY

1. Current internet service provider and connection type
 - NBN (Fibre/Cable/Fixed Wireless), Starlink, 4G/5G Mobile Broadband
2. Internet speed plan and whether it meets your business needs
 - Consider: Do you experience slow speeds during busy times?
3. Backup internet connection in case of primary failure
 - 4G/5G modem, mobile hotspot, or secondary connection
4. WiFi coverage throughout your business premises

2. EMAIL & PRODUCTIVITY TOOLS

1. Email platform and number of user accounts
 - Microsoft 365, Google Workspace, or other email service
2. Productivity suite for documents, spreadsheets, and presentations
 - Microsoft Office, Google Docs, or alternatives
3. Cloud storage solution and available capacity
 - OneDrive, Google Drive, Dropbox - Is storage sufficient?
4. Collaboration tools for team communication
 - Microsoft Teams, Slack, Zoom, or other platforms

3. DOMAINS & WEBSITES

1. All domain names owned by your business
 - *yourcompany.com.au* and any other domains
2. Domain registrar and renewal dates
 - Where domains are registered and when they expire
3. Website hosting provider and platform
 - WordPress, Wix, Squarespace, custom-built, or other

4. Website performance and mobile responsiveness
 - *Is your website fast and easy to use on phones and tablets?*
5. SSL certificate status (secure HTTPS connection)

4. SECURITY & PROTECTION

1. Antivirus and anti-malware software on all devices
 - *Windows Defender, Norton, McAfee, Bitdefender, or other*
2. Firewall protection for your network
 - *May be built into your router or separate device*
3. Password management system
 - *How passwords are stored and shared securely*
4. Multi-factor authentication (MFA) implementation
 - *Extra security step when logging in (SMS, app, or hardware key)*
5. Email security and spam filtering
 - *Protection against phishing and malicious emails*
6. Staff cybersecurity awareness and training
 - *Do employees know how to identify security threats?*
7. Incident response plan for security breaches

5. BACKUPS & DATA PROTECTION

1. Backup solution and storage location
 - *Cloud backup, external drives, or combination approach*
2. Backup frequency and automation
 - *Daily, weekly, real-time - Are backups automatic?*
3. Last time backups were tested for restoration
 - *Can you actually recover files from your backups?*
4. Offsite backup storage for disaster recovery
 - *Backups stored in different physical location*
5. Backup retention policy
 - *How long are backups kept?*

6. COMPUTERS & DEVICES

1. Number and age of desktop computers
2. Number and age of laptops
3. Company-owned mobile devices (phones and tablets)
4. Operating systems in use
 - *Windows 11, Windows 10, macOS, or mixed environment*
5. Device replacement schedule
 - *When are old computers and devices replaced?*
6. Printers, scanners, and other peripherals
7. Mobile device management (MDM) for company phones

7. SERVERS & BUSINESS APPLICATIONS

1. Server infrastructure type
 - *Cloud-based, on-premises physical server, or hybrid*
2. Key business applications and software
 - *Accounting (MYOB, Xero), CRM, industry-specific programs*
3. Where applications are hosted
 - *Cloud-based (web browser) or installed locally*
4. Software licensing and subscription management
5. Application integration and data flow between systems

8. COMPLIANCE & REGULATIONS

1. Industry-specific compliance requirements
 - *Privacy Act, GDPR, SOC2, PCI-DSS, or industry standards*
2. Type of sensitive data handled
 - *Customer information, financial records, health data, etc.*
3. Data retention and disposal policies
4. Privacy policy and data protection procedures
5. Compliance audit schedule and documentation

9. IT SUPPORT & BUDGET

1. Current IT support provider or arrangement
 - *Managed service provider, break-fix, internal staff, or none*
2. IT support response time and availability
 - *How quickly do IT issues get resolved?*
3. Monthly IT spending breakdown
 - *Internet, software licenses, support, hardware, cloud services*
4. IT budget planning and capital expenditure
5. Main IT challenges and pain points
 - *Slow systems, frequent downtime, security concerns, etc.*
6. Future IT needs and growth plans
 - *New locations, more staff, new systems, digital transformation*

Need Help With Your IT?

Contact Comm Centre for a comprehensive IT assessment and tailored solutions

We help Australian small businesses optimize their IT infrastructure